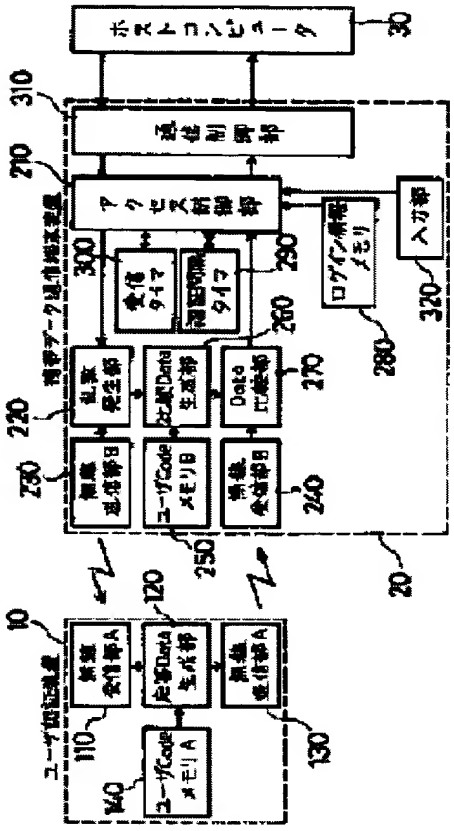
METHOD AND SYSTEM FOR USER AUTHENTICATION IN PORTABLE TYPE DATA COMMUNICATION TERMINAL

Patent number: JP2000003336
Publication date: 2000-01-07
Inventor: KATAOKA KENJI
Applicant: NEC CORP
Classification:
- international: G06F15/00; H04Q7/38; H04L9/32
- european:
Application number: JP19980167928 19980616
Priority number(s):

Also published as:
US6515575 (B1)
GB2341061 (A)

Abstract of **JP2000003336**

PROBLEM TO BE SOLVED: To provide a user authentication method and a user authentication system which can prevent an illegal use of a portable type data communication terminal by a third party.
SOLUTION: A pair is composed of a user authentication device 10 and a portable type data communication terminal 20 and a memory is made to store a user code common to each other. Then, radio communication is performed by a user log-in demand or timer management at every constant interval of time between these two devices 10 and 20 and it is confirmed that both exist in a communicable distance. Here, if both exist in the communicable distance, it is certified that the portable type data communication terminal 20 is in an appropriate use state and, only when it is certified that it is in this appropriate use state, access to a host computer 30 from the portable type data communication terminal 20 is allowed.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－3336
（P2000－3336A）
(43)公開日　平成12年１月７日(2000.1.7)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｃ	５Ｂ０８５
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｓ	５Ｋ０１３
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	５Ｋ０６７

審査請求　有　　請求項の数13　ＯＬ　（全９頁）

(21)出願番号　特願平10－167928

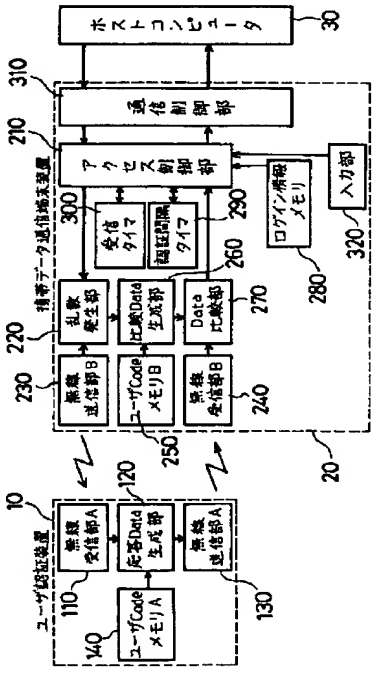
(22)出願日　平成10年６月16日(1998.6.16)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　片岡　堅治
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100089875
弁理士　野田　茂

Ｆターム(参考)　5B085 AC05 AE02 AE03 AE23 BC01
5K013 GA00 GA02
5K067 AA30 AA33 AA35 BB32 DD17
EE02 EE10 EE32 FF00 HH22

(54)【発明の名称】　携帯型データ通信端末装置におけるユーザ認証方法及びユーザ認証システム

(57)【要約】
【課題】　第３者による携帯型データ通信端末装置の不正使用を防止できるユーザ認証方法及びユーザ認証システムを提供する。
【解決手段】　ユーザ認証装置１０と携帯型データ通信端末装置２０とで１つのペアを構成し、それぞれ共通のユーザCodeをメモリに格納させておく。そして、これら２つの装置１０、２０間で、使用者のログイン要求や一定時間毎のタイマ管理によって無線通信を行い、両者が通信可能な距離に存在することを確認する。ここで、両者が通信可能な距離に存在すれば、携帯型データ通信端末装置２０が適正な使用状態にあると認証し、この適正な使用状態にあると認証した場合にだけ、携帯型データ通信端末装置２０からのホストコンピュータ３０へのアクセスを許可する。



1

【特許請求の範囲】

【請求項１】　互いに無線通信を行うための無線通信手段を有する携帯型データ通信端末装置とユーザ認証装置とを用いて前記携帯型データ通信端末装置におけるユーザ認証を行うユーザ認証方法であって、

前記携帯型データ通信端末装置と前記ユーザ認証装置との間で認証情報をやり取りすることにより、前記携帯型データ通信端末装置と前記ユーザ認証装置とが互いに前記無線通信手段の通信可能範囲内に存在することを認証し、前記携帯型データ通信端末装置の所定の動作を許可するようにした、

ことを特徴とするユーザ認証方法。

【請求項２】　前記認証情報は、ユーザに固有のコード情報であり、前記携帯型データ通信端末装置の認証情報と、前記ユーザ認証装置の認証情報の一致するか否かを判定することにより、前記認証を行うことを特徴とする請求項１記載のユーザ認証方法。

【請求項３】　前記携帯型データ通信端末装置は、ホスト装置にログイン情報をアクセスすることによって前記ホスト装置にログインする機能を有し、前記認証の結果に応じて、前記ログインを許可するか否かを決定することを特徴とする請求項１記載のユーザ認証方法。

【請求項４】　前記ログイン情報は、前記携帯型データ通信端末装置の記憶手段に予め格納され、前記記憶手段から読み出されて前記ホスト装置に送出されることを特徴とする請求項３記載のユーザ認証方法。

【請求項５】　前記ログイン情報は、ユーザの識別用のアカウント情報と認証用のパスワード情報とからなることを特徴とする請求項３記載のユーザ認証方法。

【請求項６】　前記携帯型データ通信端末装置において特定の動作要求が入力された場合に、前記認証動作を行うことを特徴とする請求項１記載のユーザ認証方法。

【請求項７】　前記認証が一旦が成立した後、一定時間間隔で認証動作を繰り返すことを特徴とする請求項６記載のユーザ認証方法。

【請求項８】　前記認証を行う場合に、携帯型データ通信端末装置からユーザ認証装置に乱数情報を含む認証要求信号を送信し、この認証要求信号を受信したユーザ認証装置で、前記乱数情報とユーザ認証装置が有する認証情報とを含む認証応答信号を生成し、この認証応答信号を携帯型データ通信端末装置に返送し、この認証応答信号を受信した携帯型データ通信端末装置において、前記応答信号から認証情報を抽出し、携帯型データ通信端末装置が有する認証情報と比較することを特徴とする請求項１記載のユーザ認証方法。

【請求項９】　携帯型データ通信端末装置とユーザ認証装置とを備えたユーザ認証システムであって、

前記携帯型データ通信端末装置及び前記ユーザ認証装置は、それぞれ自己の認証情報を記憶する記憶手段と、前記認証情報を無線によりやり取りする無線通信手段とを

2

有し、前記携帯型データ通信端末装置と前記ユーザ認証装置との間で認証情報をやり取りすることにより、前記携帯型データ通信端末装置と前記ユーザ認証装置とが互いに前記無線通信手段の通信可能範囲内に存在することを認証し、前記携帯型データ通信端末装置の所定の動作を許可するようにした、

ことを特徴とするユーザ認証システム。

【請求項１０】　前記ユーザ認証装置は、自己の認証情報を前記携帯型データ通信端末装置に無線送信する無線送信手段を有し、

前記携帯型データ通信端末装置は、前記ユーザ認証装置から認証情報を受信する無線受信手段と、受信した認証情報を自己の認証情報と比較する比較手段とを有することを特徴とする請求項９記載のユーザ認証システム。

【請求項１１】　前記携帯型データ通信端末装置は、所定の入力に基づいて前記ユーザ認証装置に認証要求を無線送信する無線送信手段を有し、

前記ユーザ認証装置は、前記携帯型データ通信端末装置からの認証要求を受信する無線受信手段を有することを特徴とする請求項１０記載のユーザ認証システム。

【請求項１２】　前記携帯型データ通信端末装置は、前記認証要求の送信後、前記ユーザ認証装置から一定時間以内に認証情報を受信するか否かを判定する計時手段を有することを特徴とする請求項１１記載のユーザ認証システム。

【請求項１３】　前記携帯型データ通信端末装置は、ホスト装置にログイン情報をアクセスすることによって前記ホスト装置にログインする機能を有するとともに、前記ログイン情報を予め記憶した記憶手段と、前記記憶手段に記憶したログイン情報を前記ホスト装置に送出するアクセス手段とを有することを特徴とする請求項９記載のユーザ認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯型データ通信端末のユーザ認証方法及びユーザ認証システムに関する。

【０００２】

【従来の技術】従来のデータ通信端末装置でホストコンピュータへログインする場合には、ホストコンピュータ側でログインを許可するための情報として、ユーザを識別するためのアカウント名と、ユーザを認証するためのパスワードを使って行われるようになっている。

【０００３】図５は、データ通信端末装置をホストコンピュータへログインするための構成例を示すブロック図である。データ通信端末装置２０でホストコンピュータ３０にログインする場合、ユーザは入力部３２０から所定の操作によるログイン要求を行う。データ通信端末装置２０のアクセス制御部２１０は、入力部３２０からのログイン要求があると、通信制御部３１を介してホスト

コンピュータ３０に接続要求を送出する。

【０００４】次に、ホストコンピュータ３０よりアカウント名とパスワードを要求されると、アクセス制御部２１０は、その旨を図示しない表示部によりユーザに通知し、その通知を受けたユーザは、入力部３２０からログイン情報４０であるアカウント名とパスワードを入力する。そして、このログイン情報４０がホストコンピュータ３０に送られ、パスワードの一致等により、ホストコンピュータ３０へのログインが実行される。

【０００５】

【発明が解決しようとする課題】しかしながら、上述のような従来の方法では、最近のように携帯型のデータ通信端末装置が普及してくるにつれて、従来の非携帯型装置では自己のオフィス内でのみ行っていたログイン情報の入力を、オフィス以外の場所で行う場合が多くなってくるため、このログイン情報の入力を第３者に盗み見られる危険が大きくなる。また、データ通信端末装置が携帯可能になると、従来の非携帯型装置ではなかったデータ通信端末装置自体の盗難や紛失の可能性も大きくなる。

【０００６】そこで本発明の目的は、第３者による携帯型データ通信端末装置の不正使用を防止できるユーザ認証方法及びユーザ認証システムを提供することにある。

【０００７】

【課題を解決するための手段】本発明は前記目的を達成するため、互いに無線通信を行うための無線通信手段を有する携帯型データ通信端末装置とユーザ認証装置とを用いて前記携帯型データ通信端末装置におけるユーザ認証を行うユーザ認証方法であって、前記携帯型データ通信端末装置と前記ユーザ認証装置との間で認証情報をやり取りすることにより、前記携帯型データ通信端末装置と前記ユーザ認証装置とが互いに前記無線通信手段の通信可能範囲内に存在することを認証し、前記携帯型データ通信端末装置の所定の動作を許可するようにしたことを特徴とする。

【０００８】また本発明は、携帯型データ通信端末装置とユーザ認証装置とを備えたユーザ認証システムであって、前記携帯型データ通信端末装置及び前記ユーザ認証装置は、それぞれ自己の認証情報を記憶する記憶手段と、前記認証情報を無線によりやり取りする無線通信手段とを有し、前記携帯型データ通信端末装置と前記ユーザ認証装置との間で認証情報をやり取りすることにより、前記携帯型データ通信端末装置と前記ユーザ認証装置とが互いに前記無線通信手段の通信可能範囲内に存在することを認証し、前記携帯型データ通信端末装置の所定の動作を許可するようにしたことを特徴とする。

【０００９】本発明のユーザ認証方法及びユーザ認証システムにおいて、携帯型データ通信端末装置とユーザ認証装置は２つ１組で構成され、互いに無線通信を行う手段を有する。そして、携帯型データ通信端末装置とユーザ認証装置は、それぞれ認証情報を保持しており、この認証情報を携帯型データ通信端末装置とユーザ認証装置との間で無線通信によりやり取りすることで、両者が互いに通信可能範囲内に存在することを認証する。そして、この認証が成功した場合にだけ、携帯型データ通信端末装置の所定の動作、例えばホストコンピュータへのログインを許可する。また、認証が不成功の場合には、携帯型データ通信端末装置がユーザ認証装置より離れた場所で第３者によって不正に使用されている可能性があると判断し、携帯型データ通信端末装置の動作を制限する。これにより、携帯型データ通信端末装置の第３者による不正使用を防止できる。

【００１０】

【発明の実施の形態】以下、本発明によるユーザ認証方法及びユーザ認証システムの実施の形態について説明する。図１は、本発明によるユーザ認証システムの一例を示すブロック図である。図１に示すように、本例のユーザ認証システムは、ユーザ認証装置１０と携帯型データ通信端末装置２０とで１つのペアを構成し、これら２つの装置１０、２０間で、使用者のログイン要求や一定時間毎のタイマ管理によって無線通信を行い、両者が通信可能な距離に存在することを確認することで、携帯型データ通信端末装置２０が適正な使用状態にあると認証するものであり、この適正な使用状態にあると認証した場合にだけ、携帯型データ通信端末装置２０からのホストコンピュータ３０へのアクセスを許可するものである。

【００１１】ユーザ認証装置１０は、無線受信部Ａ１１０と、応答Data生成部１２０と、無線送信部Ａ１３０と、ユーザCodeメモリ１４０とを有する。無線受信部Ａ１１０は、携帯型データ通信端末装置２０からの認証要求信号を受信し、認証要求信号の中から乱数Dataを取り出して応答Data生成部１２０に出力する。ユーザCodeメモリＡ１４は、ユーザ認証装置１０が有しているユーザCodeを記憶したものであり、このユーザCodeを応答Data生成部１２０に出力する。応答Data生成部１２０は、無線受信部Ａ１１０より入力された乱数DataとユーザCodeメモリ１４０より入力されたユーザCodeを用いて、応答Dataを生成し、無線送信部Ａ１３０に出力する。無線送信部Ａ１３０は、応答Data生成部１２０より入力された応答Dataから認証応答信号を生成し、無線信号によって携帯型データ通信端末装置２０に送信する。

【００１２】一方、携帯型データ通信端末装置２０は、アクセス制御部２１０と、乱数発生部２２０と、無線送信部Ｂ２３０と、無線受信部Ｂ２４０と、ユーザCodeメモリＢ２５０と、比較Data生成部２６０と、Data比較部２７０と、ログイン情報メモリ２８０と、認証間隔タイマ２９０と、受信タイマ３００と、通信制御部３１０と、入力部３２０とを有する。アクセス制御部２１０は、入力部３２０からのログイン要求に応じて、アクセスするホストコンピュータ３０へのログイン・ログアウ

ト処理を制御するものであり、通信制御部３１０は、ホストコンピュータ３０への実際の通信動作を司るものである。乱数発生部２２０は、アクセス制御部２１０からの指示により乱数を発生し、無線送信部Ｂ２３０及び比較Data生成部２６０に対して乱数Dataを出力する。

【００１３】無線送信部Ｂ２３０は、乱数発生部２２０より入力された乱数Dataから認証要求信号を生成し、無線信号によって送信する。無線受信部Ｂ２４０は、ユーザ認証装置１０からの認証応答信号を受信し、認証応答信号の中から応答Dataを取り出してData比較部２７０に出力する。ユーザCodeメモリＢ２５０は、ユーザ認証装置１０の有するものと同一のユーザCodeを記憶したものであり、比較Data生成部２６０に対して、ユーザCodeを出力する。

【００１４】比較Data生成部２６０は、乱数発生部２２０から入力された乱数DataとユーザCodeメモリＢ２５０から入力されたユーザCodeとを用いて、比較Dataを生成し、Data比較部２７０に出力する。Data比較部２７０は、比較Data生成部２６０から入力された比較Dataと、無線受信部Ｂ２４０から入力された応答Dataとを比較し、その結果をアクセス制御部２１０に出力する。受信タイマ３００は、アクセス制御部２１０が乱数発生部２２０に指示を出した直後からカウントを開始し、一定時間経過しても認証応答信号が受信されなかった場合に、アクセス制御部２１０へタイムアウトを通知する。ログイン情報メモリ２８０は、ホストコンピュータ３０にログインするために必要な情報がメモリされており、アクセス制御部２１０からの要求により、ログイン情報を出力する。

【００１５】認証間隔タイマ２９０は、一旦、ログインが認証された後から計時のカウントを開始し、ログイン時と同じ認証通信をユーザ認証装置１０に対して一定間隔毎に行うためのタイマであり、タイムアウト時には、その旨をアクセス制御部２１０へ通知する。この通知に対してアクセス制御部２１０は、Data比較部２７０からの比較結果を入力することにより、比較結果が一致なら認証可（以下、認証ＯＫという）として、ログイン情報メモリ２８０より、ログインに必要な情報を読み出し通信制御部３１０に出力して、ホストコンピュータ３０へのログインを行う。また、比較結果が不一致および受信タイマ３００がタイムアウトした場合には、アクセス制御部２１０は認証不可（以下、認証ＮＧという）として、通信制御部３１０に対して切断要求を出力し、ホストコンピュータ３０との接続を切る。

【００１６】以上のように認証間隔タイマ２９０によって認証動作を行う間隔としては、通信中にユーザ認証装置１０を持ったユーザが携帯型データ通信端末装置２０から離れた際に他人から使用されないようにすることを考慮した場合には、例えば１０秒程度が適当である。ただし、ユーザが席を離れた場合の安全性は、使用するユーザの事情により異なることから、比較的安全性が高い場合には、１分程度であってもよいことが考えられる。また、このような認証時間をユーザが所定の操作を行うことで、認証間隔タイマ２９０に可変設定できるようにしてもよい。また、ユーザ認証装置１０と携帯型データ通信端末装置２０との無線通信可能な範囲についても、ユーザの使用環境によって種々考えられるが、例えば数ｍ～十数ｍの範囲で設定できる。また、例えばユーザ認証装置１０における無線送信部Ａ１３０の送信出力を可変設定可能に構成し、ユーザが適宜選択できるようにしてもよい。

【００１７】また、本例において使用するデータ通信の信号フォーマットは、例えば携帯電話（ＰＤＣ方式）やＰＨＳ（パーソナルハンディホンシステム）等の標準規格（ＲＣＲＳＴＤ－２７、２８）を用いるものとする。ただし、信号フォーマットとしては、本システムを使用する地域等の通信インフラに依存して、各種のものを採用し得るものである。また、ユーザCodeとしては、長ければ長いほど、セキュリティの面では強固になる。また、本システムでは、番号の重複は許されない。しかしながら、長過ぎても計算等の時間が長くなってしまう。そこで、一般的には、本例の機能を有する端末が十分普及しても、番号の重複を生じない程度に必要十分な長さを選択することになる。具体的には、２進数で６４桁程度を採用する。また、このようなユーザCodeを格納するメモリＡ１４、メモリＢ２５には、ＲＯＭを用いればよい。

【００１８】次に、以上のようなシステムにおけるデータ認証方法について図２～図４のフローチャートに従い説明する。図２は、本例におけるユーザ認証装置１０の動作を示すフローチャートである。また、図３、図４は、本例における携帯型データ通信端末装置２０の動作を示すフローチャートであり、図３は主にアクセス制御部２１０の動作を示し、図４は、特にユーザ認証装置１０と携帯型データ通信端末装置２０との間で行う認証通信の動作について示している。

【００１９】まず、図２において、ユーザ認証装置１０は、電源投入後、通常受信待ちの状態にあって、携帯型データ通信端末装置２０からの認証要求信号を待ち受けており、無線受信部Ａ１１０にて受信ありかどうかをチェックし（ステップＳ２０１）、受信がない場合（ステップＳ２０２）には、受信信号有無のチェックを繰り返す（ステップＳ２０３）。また、受信ありの場合（ステップＳ２０４）には、無線受信部Ａ１１０にて、受信した認証要求信号から乱数Dataを取り出し（ステップＳ２０５）、応答Data生成部１２０へ出力する（ステップＳ２０６）。応答Data生成部１２０は、ユーザCodeメモリＡ１４からユーザCodeを読み出し（ステップＳ２０７）、乱数DataとユーザCodeから応答Dataを生成し（ステップＳ２０８）、無線送信部Ａ１３０に出力する（ス

テップＳ２０９）。無線送信部Ａ１３０は、応答Data生成部１２０から入力された応答Dataより、認証応答信号を生成し（ステップＳ２１０）、無線信号にて送信する（ステップＳ２１１）。送信後は、再び受信待ち状態に戻る（ステップＳ２０３）。

【００２０】一方、図３において、携帯型データ通信端末装置２０は、電源投入後、通常ログイン要求待ちの状態にあって、入力部３２０からの入力を待ち受けており、入力部３２０からのログイン要求があるかどうかをチェックし（ステップＳ３０１）、ログイン要求がない場合（ステップＳ３０２）には、ログイン要求有無のチェックを繰り返す（ステップＳ３０３）。ログイン要求ありの場合（ステップＳ３０４）には、認証確認（ステップＳ４００）を行い、ユーザ認証装置１０との通信の成否による認証を確認する（ステップＳ３０５）。認証確認（ステップＳ４００）の処理については、図４にて説明する。ここで、認証ＮＧ（ステップＳ３０６）ならば、再びログイン要求待ち状態に戻る（ステップＳ３０３）。

【００２１】認証ＯＫ（ステップＳ３０７）ならば、アクセス制御部２１０は、ログイン情報メモリ２８０からログイン情報を読み出し（ステップＳ３０８）、その情報を通信制御部３１０へ出力し（ステップＳ３０９）、ホストコンピュータ３０へログインする（ステップＳ３１０）。ログイン後は、アクセス制御部２１０の指示により、認証間隔タイマ２９０を開始し（ステップＳ３１２）、次の認証確認までのタイムアウト待ち状態となり、タイムアウトをチェックする（ステップＳ３１４）。タイムアウトでない場合（ステップＳ３１５）は、入力部３２０からのログアウト要求の有無をチェックし（ステップＳ３１７）、ログアウト要求がなければ（ステップＳ３１８）、認証間隔タイマ２９０のタイムアウトチェックへ戻る（ステップＳ３１３）。また、ログアウト要求があれば（ステップＳ３１９）、認証間隔タイマ２９０を解除し（ステップＳ３２０）、認証ＮＧの場合と同様の処理を行う（ステップＳ３２４）。

【００２２】また、認証間隔タイマ２９０がタイムアウトした場合（ステップＳ３１６）には、再び認証確認（ステップＳ４００）を行い、ユーザ認証装置との通信の成否による認証を確認する（ステップＳ３２１）。ここで、認証ＯＫ（ステップＳ３２２）ならば、そのまま再度認証確認タイマ２９でのループを繰り返す（ステップＳ３１１）。認証ＮＧ（ステップＳ３２３）ならば、アクセス制御部２１０は、通信制御部３１０に対して切断要求を出し（ステップＳ３２５）、ホストコンピュータ３０からログアウトし（ステップＳ３２６）、再び入力部３２０からのログイン要求待ち受け状態に戻る（ステップＳ３０３）。

【００２３】図４において、認証確認（ステップＳ４００）では、まず、アクセス制御部２１０からの指示で、乱数発生部２２０にて乱数Dataを発生させて無線送信部Ｂ２３０へ出力する（ステップＳ４０１）。無線送信部Ｂ２３０は、乱数発生部２２０から入力された乱数Dataより、認証要求信号を生成し（ステップＳ４０２）、無線信号にて送信する（ステップＳ４０３）。送信後は、アクセス制御部２１０の指示により、受信待ち受けのリミット時間である受信タイマ３００の計時を開始し（ステップＳ４０４）、認証応答信号の待ち受け状態に入る。

【００２４】そして、この待ち受け状態中は、無線受信部Ｂ２４０で受信ありかどうかをチェックし（ステップＳ４０６）、受信がない場合（ステップＳ４０７）には、受信タイマ３００のタイムアウトをチェックし（ステップＳ４０９）、タイムアウトでなければ（ステップＳ４１０）、受信信号有無のチェックを繰り返す（ステップＳ４０５）。また、受信ありの場合（ステップＳ４０８）には、無線受信部Ｂ２４０は受信した認証応答信号から応答Dataを取り出し（ステップＳ４１４）、Data比較部２７０へ出力する（ステップＳ４１５）。また、比較Data生成部２６０は、乱数発生部２２０から入力された（ステップＳ４１６）乱数Dataと、ユーザCodeメモリＢ２５０から読み出した（ステップＳ４１７）ユーザCodeを使用して、比較Dataを生成し（ステップＳ４１８）、Data比較部２７０へ出力する（ステップＳ４１９）。

【００２５】ここで、Data比較部２７０は、無線受信部Ｂ２４０から入力された応答Dataと、比較Data生成部２６０から入力された比較Dataとを比較し（ステップＳ４２０）、一致していた場合（ステップＳ４２２）には、認証ＯＫとし（ステップＳ４２３）、不一致だった場合（ステップＳ４２１）には、認証ＮＧ（ステップＳ４１３）とする。そして、認証判定終了後は、受信タイマ３００を解除して（ステップＳ４２５）、認証確認を終了する（ステップＳ４２６）。また、受信タイマ３００がタイムアウトした場合（ステップＳ４１１）は、比較Dataと応答Dataが不一致の場合と同様の処理（ステップＳ４１２）を行う。

【００２６】以上のような本例によれば、携帯型データ通信端末装置２０において、ユーザ認証装置１０と携帯型データ通信端末装置２０の両方を揃えないと、ホストコンピュータ３０へのアクセスができなくなるため、盗難や紛失による第３者からのホストコンピュータ３０に対する不正アクセスのセキュリティを向上することができる。また、本例では、無線通信を利用して非接触で認証を行うため、ユーザ認証装置１０と携帯型データ通信端末装置２０を別々に持ち歩くことができ、同時に紛失や盗難にあう可能性を少なくすることができる。

【００２７】さらに、無線通信で認証を行うため、ユーザ認証装置１０と携帯型データ通信端末装置２０との距離が離れると認証ＮＧとなり、ユーザ認証装置１０を持

ったユーザが一時的に携帯型データ通信端末装置２０の側を離れているような場合にも、携帯型データ通信端末装置２０によるホストコンピュータ３０へのアクセスは阻止でき、セキュリティが保護される。さらに、乱数を利用して毎回認証通信の内容を変更しているので、無線区間での盗聴に対しても保護される。

【００２８】また、本例では、認証を行う際に、予めログイン情報メモリ２８０に記憶したログイン情報を送出することから、その都度ユーザがログイン情報を入力する必要がない。このため、携帯型データ通信端末装置２０をオフィス外等で使用して、ホストコンピュータ３０にログインする場合にも、ログイン情報を盗み見られることがなくなる効果がある。また、認証に要する時間を短縮でき、また、操作を簡素化することができる効果もある。

【００２９】なお、以上の例では、認証の結果により制限する携帯型データ通信端末装置２０の動作として、ホストコンピュータ３０へのログインを制限する場合について説明したが、他の動作を制限するものであってもよい。

【００３０】

【発明の効果】以上説明したように本発明のユーザ認証方法では、携帯型データ通信端末装置とユーザ認証装置との間で無線通信によって認証情報をやり取りすることで、携帯型データ通信端末装置とユーザ認証装置とが互いに無線通信可能な範囲内に存在することを認証し、携帯型データ通信端末装置の所定の動作を許可するようにした。このため、携帯型データ通信端末装置とユーザ認証装置の双方を所有する適正な使用者が携帯型データ通信端末装置を使用する場合にだけ、携帯型データ通信端末装置の動作を許可することができ、携帯型データ通信端末装置の第３者による不正使用を防止できる効果がある。

【００３１】また本発明のユーザ認証システムでは、携＊帯型データ通信端末装置とユーザ認証装置との間で無線通信によって認証情報をやり取りすることで、携帯型データ通信端末装置とユーザ認証装置とが互いに無線通信可能な範囲内に存在することを認証し、携帯型データ通信端末装置の所定の動作を許可するようにした。このため、携帯型データ通信端末装置とユーザ認証装置の双方を所有する適正な使用者が携帯型データ通信端末装置を使用する場合にだけ、携帯型データ通信端末装置の動作を許可することができ、携帯型データ通信端末装置の第３者による不正使用を防止できる効果がある。

【図面の簡単な説明】

【図１】本発明によるユーザ認証システムの構成例を示すブロック図である。

【図２】図１に示すユーザ認証システムにおけるユーザ認証装置の動作を示すフローチャートである。

【図３】図１に示すユーザ認証システムにおける携帯型データ通信端末装置の動作を示すフローチャートである。

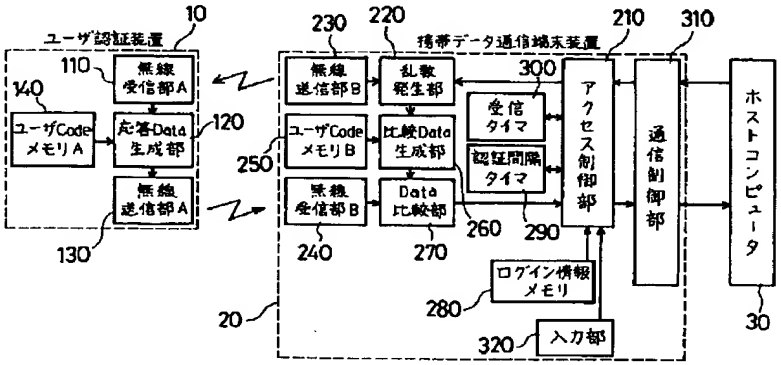
【図４】図１に示すユーザ認証システムにおける認証通信動作を示すフローチャートである。

【図５】従来の携帯型データ通信端末装置とホストコンピュータを用いたシステムの構成例を示すブロック図である。

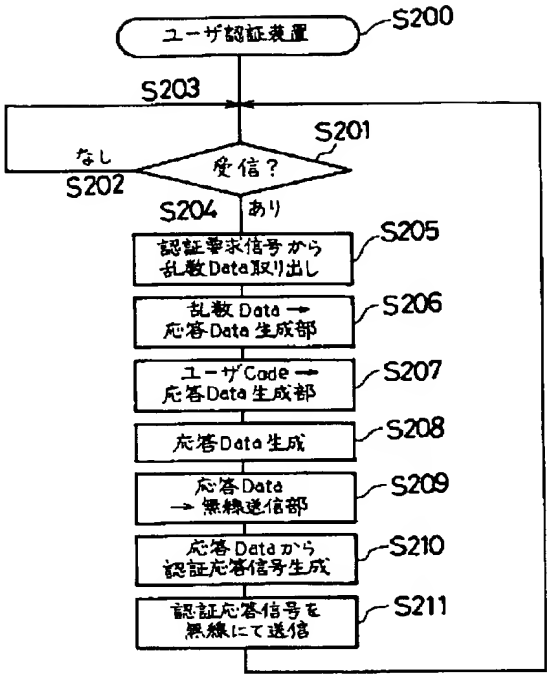
【符号の説明】

１０……ユーザ認証装置、２０……携帯型データ通信端末装置、３０……ホストコンピュータ、１１０……無線受信部Ａ、１２０……応答Data生成部、１３０……無線送信部Ａ、１４０……ユーザCodeメモリ、２１０……アクセス制御部、２２０……乱数発生部、２３０……無線送信部Ｂ、２４０……無線受信部Ｂ、２５０……ユーザCodeメモリＢ、２６０……比較Data生成部、２７０……Data比較部、２８０……ログイン情報メモリ、２９０……認証間隔タイマ、３００……受信タイマ、３１０……通信制御部、３２０……入力部。

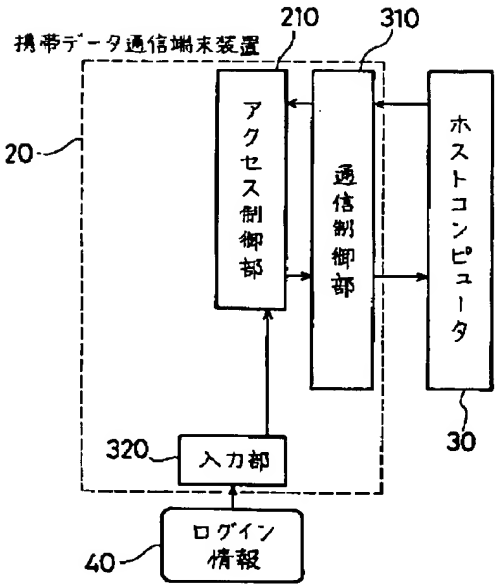
【図１】



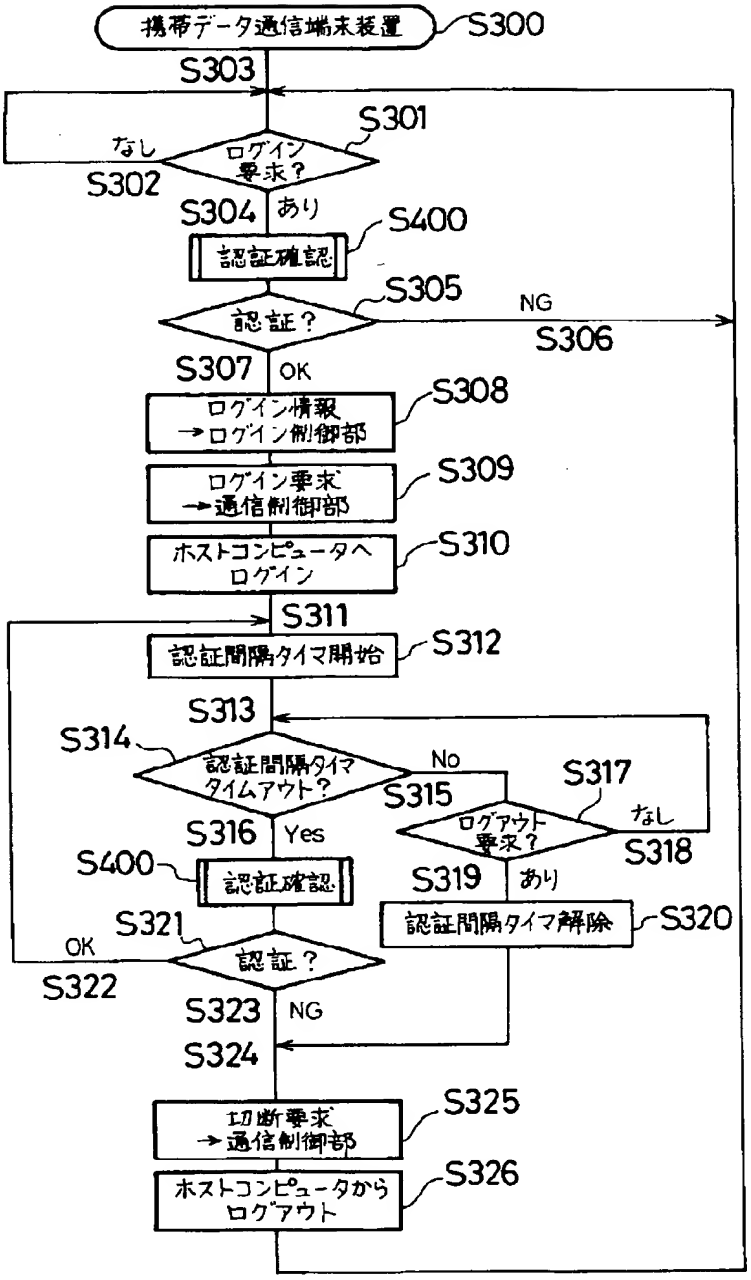
【図２】


ユーザ認証装置
S200
S203
S201
受信？
なし
S202
S204
あり
認証要求信号から乱数Data取り出し
S205
乱数Data→応答Data生成部
S206
ユーザCode→応答Data生成部
S207
応答Data生成
S208
応答Data→無線送信部
S209
応答Dataから認証応答信号生成
S210
認証応答信号を無線にて送信
S211

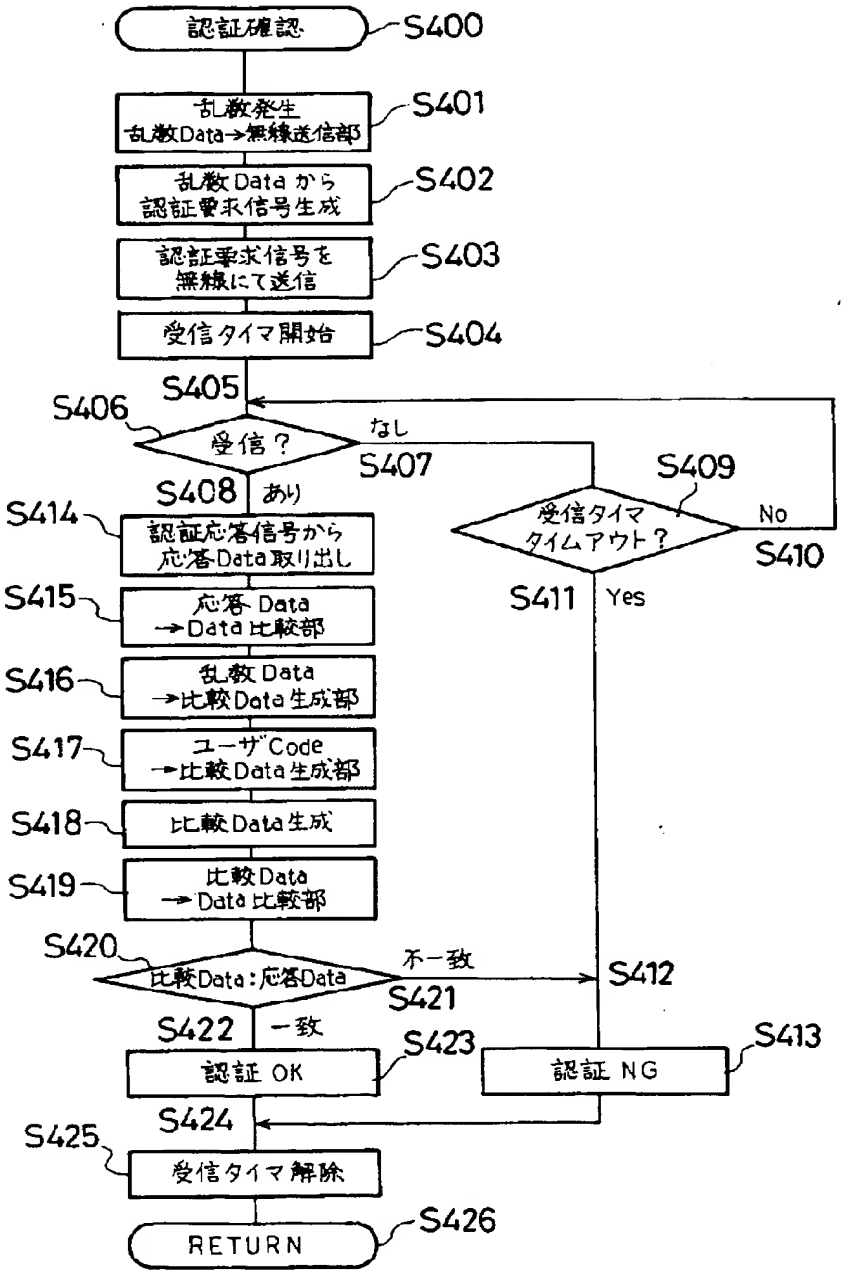
【図５】


携帯データ通信端末装置
210
310
20
アクセス制御部
通信制御部
ホストコンピュータ
30
320
入力部
ログイン情報
40

【図３】


携帯データ通信端末装置
S300
S303
S301
なし
ログイン要求？
S302
S304
あり
S400
認証確認
S305
認証？
NG
S306
S307
OK
S308
ログイン情報→ログイン制御部
S309
ログイン要求→通信制御部
S310
ホストコンピュータへログイン
S311
S312
認証間隔タイマ開始
S313
S314
認証間隔タイマタイムアウト？
No
S315
S317
ログアウト要求？
なし
S318
S316
Yes
S400
認証確認
S319
あり
S320
認証間隔タイマ解除
S321
OK
認証？
S322
S323
NG
S324
S325
切断要求→通信制御部
S326
ホストコンピュータからログアウト

【図４】


認証確認
S400
乱数発生
乱数Data→無線送信部
S401
乱数Dataから
認証要求信号生成
S402
認証要求信号を
無線にて送信
S403
受信タイマ開始
S404
S405
S406
受信？
なし
S407
S409
受信タイマ
タイムアウト？
No
S410
S408
あり
S411
Yes
S414
認証応答信号から
応答Data取り出し
S415
応答Data
→Data比較部
S416
乱数Data
→比較Data生成部
S417
ユーザCode
→比較Data生成部
S418
比較Data生成
S419
比較Data
→Data比較部
S420
比較Data：応答Data
不一致
S421
S412
S422
一致
S423
認証OK
認証NG
S413
S424
S425
受信タイマ解除
RETURN
S426